IN THE CLAIMS:

The following is a complete listing of claims in this application.

Claims 1-94 (canceled).

95. (currently amended) A protection system for a computerized device comprising an operating system, and at least one peripheral device selected from the group consisting of at least one storage device, and at least one communication device, the protection system comprising:

a monitoring and capturing sub-system configured to monitor activities relating to said at least one storage ~~devices~~ device and said at least one communication ~~peripherals~~ device, and to detect and to act against suspicious or dangerous activity; ~~and~~

an encrypted database in operative connection with said operating system, and storing default security rules including default rules, pre distribution rules, additionally-acquired user-defined rules, and statistics of acceptable program behavior continuously learned during system operation,

said monitoring and capturing sub-system being constructed and arranged to receive data from said encrypted database, and to block activities of said computerized device in violation of said default rules; and

a user interface operatively connected to said operating system, and including means for performing at least one function selected from the group consisting of learning acceptable behavior patterns to be added to said database, warning the user of perceived dangers based on said database and requesting user authorization to perform an action.

wherein accesses to the encrypted database is tracked by the monitoring and capturing sub-system.

96. (currently amended) The system of claim 95, wherein

the encrypted database further stores a log of security questions presented to ~~users~~ the user and replies thereto.

97. (previously presented) The system of claim 95, wherein the encrypted database further stores a log of detected suspicious activities.

98. (withdrawn) A method of monitoring, checking and authorizing access to hooked functions that are called due to a memory-related action, the method comprising:

retrieving the identity of the entity calling the hooked function;

retrieving related information from a database;

receiving the hooked function's parts and self-allocated memory;

checking if memory limits are exceeded; and

passing parameters to the original hooked function if the memory limits are not exceeded.

99. (withdrawn) The method of claim 98, wherein, if the memory limits are exceeded, the method further comprises:

requesting permission from a user as a condition to passing parameters to the original hooked function.

100. (withdrawn) The method of claim 98, wherein, if the memory limits are exceeded, the method further comprises:

terminating a process that called the hooked function.

101. (withdrawn) The method of claim 98, wherein, if the memory limits are exceeded, the method further comprises:

falsely indicating that a request that called the hooked function has been completed.